# CS70 Discussion 2d Review

Agnibho Roy

Summer 2020

## 1 Review

These are just concepts and strategies discussed during discussion section on July 2, 2020. For definitions and formulas, refer to note 7 on the course website.

### 1.1 Modular Arithmetic

- Modular Arithmetic is a way for us to look at computation in a specific range of integers from 0 to $m-1$ if we are looking in the modular space $m$.
- The term $x \equiv r \pmod{m}$ means nothing but, if we take some number $x$ and divide by $m$, then we will get the remainder $r$. A common way to move from the modular to the non-modular world is by the representation of the previous equation as $x = qm + r$ for some $q \in Z$.
- Product rule of modular arithmetic (very good for simplifying computation): $a * b \pmod{m} = a \pmod{m} * b \pmod{m}$. The same works for addition as well.
- gcd algorithm: $\gcd(x, y) = \gcd(y, x \pmod{y})$.
- There exists no division in modular arithmetic as we would describe it in the real world, but rather a multiplicative inverse, which is defined as some $b$ for which $a * b = 1 \pmod{m}$. This exists if and only if $\gcd(a, m) = 1$. The inverse can be iteratively guessed or calculated by the egcd algorithm.

## 2 Extra Problems

These problems are not necessarily in scope. Some may be helpful on exams, but some others are just fun exercises. Reach out to me by email (agnibhoroy@berkeley.edu) if you see any mistakes or have questions about any of the questions.

### 2.1 Simplify

Simplify the following to a value $0 \le x < m$ for expressions in modulo $m$

1. $7^{2020} \pmod{50}$    2020 → $(7^a)^b$ → $7^a$ simple (mod 50)
2. $1! + 2! + 3! \dots 200! \pmod{24}$

### 2.2 Fall 2018 Modular Question

Let a sequence of psuedo-random numbers be $x_1, x_2, \dots x_n$ and the sequence is recursively defined as $x_n \equiv a x_{n-1}$ Here $p$ is a prime number, $a$ is a positive integer such that $a \not\equiv 0 (\text{mod} p)$, and $x_0 \in Z^+$ is a seed (initialization) satisfying $x_0, a \not\equiv 0 (\text{mod} p)$. The period $d$ is the smallest $n \in Z^+$ such that $x_n \equiv x_0 (\text{mod} p)$; note that the sequence repeats after $d$ numbers have been generated. We want to make $d$ as large as possible.

1. for $n \in N$, find $x_n$ as a function of $n, a, \text{and} x_0$.
2. Prove that $a^d \equiv 1 \pmod{p}$
3. Let $n_0$ be the smallest positive integer $n$ such that $a^{\cancel{x}\,n} \equiv 1 \pmod{p}$. Prove that $n_0$ divides all positive integers $n$ such that $a^n \equiv 1 \pmod{p}$.
4. Finally prove that the period $d$ divides $p - 1$. State clearly which results you used to prove this claim.

1) $7^{2020} \pmod{50} = (7^2)^{1010} = 49^{1010} = (-1)^{1010} = 1 \pmod{50}$

$49 \equiv -1 \pmod{50}$

2) $1! + 2! + 3! \ldots 200! \pmod{24} \equiv 1! + 2! + 3! = 1+2+6 = 9 \pmod{24}$

$4! = 24$

$5! = 5 \cdot \cancel{4!}^{\,0} \pmod{24}$ $\qquad 10! = 10 \cdot 9 \cdot 8 \cdot 7 \cdots 5 \cdot \cancel{4!}^{\,0}$

$5! \equiv 0 \pmod{24}$

any $n \geq 4$: $n(n-1)(n-2)\ldots(4!)$

for any $n \geq 4$: $n! \equiv 0 \pmod{24}$

2.2) 1) $x_n = a x_{n-1}$

$x_1 = a x_0$

$x_2 = a x_1 \rightarrow x_2 = a(a x_0) = a^2 x_0 = x_n = \overbrace{a(a(a \ldots x_0)}^{n \text{ times}} =$

$x_n = a^n x_0 \pmod{p}$

2) $x_d \equiv x_0 \pmod{p}$ $\qquad \gcd(x_0, p) = 1$

$x_d = a^d x_0 \pmod{p}$

$a^d x_0 = x_0 \pmod{p}$

$a^d \cancel{x_0 (x_0^{-1}} \pmod{p}) = \cancel{x_0 (x_0^{-1}} \pmod{p}) \pmod{p}$

$\underline{a^d \equiv 1 \pmod{p}}$

3) $\exists\, n_0$ s.t. $a^{n_0} \equiv 1 \pmod{p}$

$\exists\, n'$ s.t. $n' > n_0$, $\underline{a^{n'} \equiv 1} \pmod{p}$

goal $\rightarrow$ $n_0 \mid n'$

$\underline{n' = q n_0 + r}$ for some $q \in \mathbb{Z}$ $\longrightarrow$ $n' = q n_0 \rightarrow \boxed{n_0 \mid n'}$

goal $\rightarrow r = 0$

$a^{q n_0 + r} \equiv 1 \pmod{p}$

$$a^{q n_0} a^r \equiv 1 \pmod p$$

$$(\cancel{a}^{n_0})^q a^r \equiv 1 \pmod p$$

$r = 0 \Rightarrow (a^{n_0})^q \equiv 1 \pmod p$ $\quad 1^q \equiv 1$

$a^r \equiv 1 \pmod p \rightarrow$ contradiction $r < n_0$ & we assumed that $n_0$ is the smallest # that satisfies $a^n \equiv 1 \pmod p$

$r = 0$

iv) $a^d \equiv 1 \pmod p$ $\qquad a^{n_0} \equiv 1 \pmod p$

$d$ is smallest possible value $\qquad \downarrow$

$a^{p-1} \equiv 1 \pmod p$ $\qquad a^{n'} \equiv 1 \pmod p$

$d \mid p-1$ $\qquad n_0 \mid n'$

## Vitamin 2.2

$$\begin{cases} b \equiv 3 \pmod{11} \\ b \equiv 0 \pmod{13} \end{cases} \rightarrow 13 \mid b$$

CRT setup